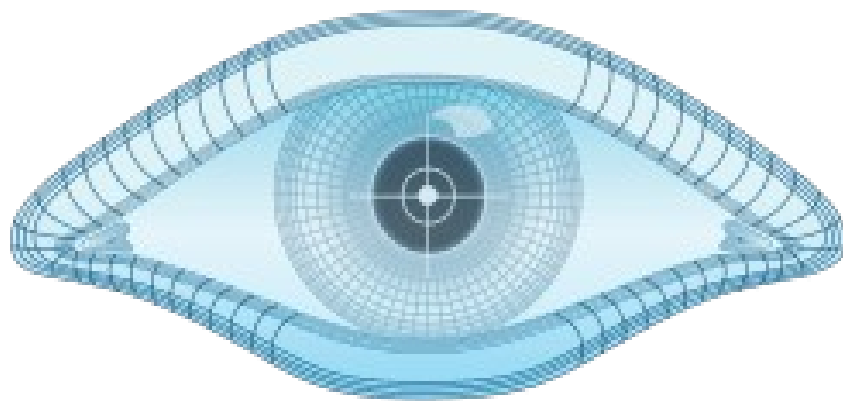


UD1_T3.1 Disponibilidad NMAP



NMAP

Nicolás González Dobarro

Índice

EJERCICIO 1 - Escanear puertos abiertos en localhost.....	3
(en terminal y Zenmap).....	3
EJERCICIO 2 - Instalar servidores comprobar que se abren nuevos puertos.....	6
EJERCICIO 3 - Comprobar los hosts activos de la red.....	9
(envía pings).....	9
EJERCICIO 4 - Comprobar los puertos abiertos.....	10
en un host de la red.....	10
EJERCICIO 5 - Comprobar las versiones de los servicios que se ejecutan en los puertos.....	10
EJERCICIO 6 - Detectar S.O.....	11

EJERCICIO 1 - Escanear puertos abiertos en localhost

(en terminal y Zenmap)

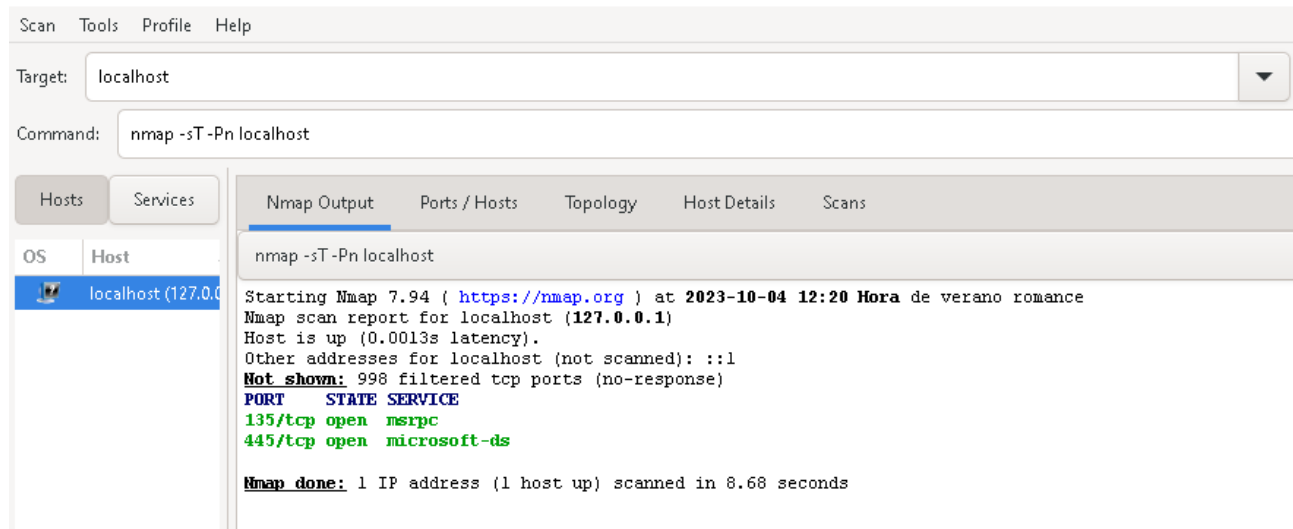
WINDOWS (tcp sin ping)

> nmap -sT -Pn localhost (-sT: SYN y RST)

-> Comprueba los puertos/servicios abiertos en <https://www.speedguide.net/port.php>

Comenta para qué se utiliza cada puerto/servicio abierto.

Recurso: <https://www.speedguide.net/ports.php>



El puerto TCP 445 se utiliza para acceso directo a redes TCP/IP MS sin necesidad de una capa NetBIOS.

El puerto 135 de llamada a procedimiento remoto (RPC) se utiliza en aplicaciones cliente/servidor.

-> ¿Qué problemas de seguridad tiene el tener abierto el puerto 445?

Dejar el puerto 445 abierto deja a las máquinas Windows vulnerables a una serie de troyanos y gusanos:

W32.HLLW.Deloder

IraqiWorm

W32.HLLW.Moeg

W32.Korgo.AB

Backdoor.Rtkit.B

W32.Sasser .Gusano

Trojan.Netdepix.B

Backdoor.IRC.Cirebot

-> ¿Qué servicio dejará de funcionar si bloqueamos el puerto 445 en el firewall?

El servicio de compartición de archivos o impresoras en la LAN.

-> ¿Qué problemas de seguridad tiene el tener abierto el puerto 5357?

El puerto 5357 provee un servicio poco fidedigno y datagramas pueden llegar en duplicado, descompuestos o perdidos sin aviso.

LINUX

> nmap localhost

> nmap 127.0.0.1

```
root@usuario:/home/usuario# nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-04 12:50 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
631/tcp   open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@usuario:/home/usuario# nmap 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-04 12:50 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
631/tcp   open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@usuario:/home/usuario#
```

EJERCICIO 2 - Instalar servidores comprobar que se abren nuevos puertos

WINDOWS

- Instalar XAMPP, que posee las siguientes herramientas:

SERVIDORES

SQL: MySQL - MariaDB (versión GPL MySQL)

Web: Apache, Tomcat

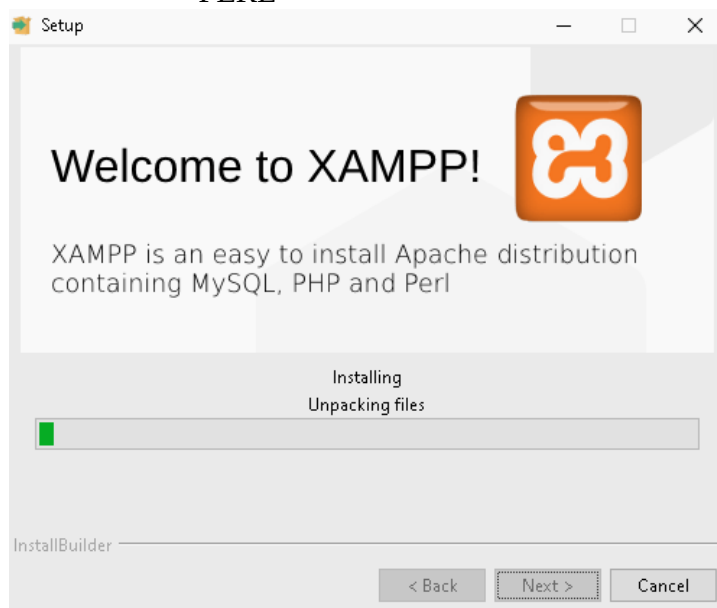
FTP: FileZilla

Mail: Mercury

INTÉRPRETES LENGUAJES

PHP

PERL



-> Activa los servidores MySQL y Apache

XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]



-> Vuelve a escanear los puertos abiertos en localhost

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-05 17:11 Hora de verano romance
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00091s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 95 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
443/tcp    open  https
445/tcp    open  microsoft-ds
3306/tcp   open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

-> ¿Qué nuevos puertos se han abierto? ¿A qué servidor corresponde cada uno?

LINUX - Instalar Apache:

> sudo apt-get install apache2

```
root@usuario:/home/usuario# apt-get install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Paquetes sugeridos:
 apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Se instalarán los siguientes paquetes NUEVOS:
 apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 actualizados, 8 nuevos se instalarán, 0 para eliminar y 4 no actualizados.
Se necesita descargar 1.918 kB de archivos.
Se utilizarán 7.706 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

> sudo service apache2 start/restart/stop/status

-> Inicia el servidor Apache

```
root@usuario:/home/usuario# service apache2 start
```

-> Vuelve a escanear los puertos abiertos en localhost

```
root@usuario:/home/usuario# service apache2 start
root@usuario:/home/usuario# nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-05 16:58 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
631/tcp    open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

-> ¿Qué nuevo puerto se ha abierto?

El puerto 80, del servidor web Apache.

-> Detén el servidor Apache

```
root@usuario:/home/usuario# service apache2 stop
```

-> Vuelve a escanear los puertos abiertos en localhost

```
root@usuario:/home/usuario# service apache2 stop
root@usuario:/home/usuario# nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-05 17:05 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
631/tcp    open  ipp
```

EJERCICIO 3 - Comprobar los hosts activos de la red (envía pings)

```
> nmap -sP W.X.Y.*  
> nmap -sP W.X.Y.Z/M (Desde ubuntu)
```

```
root@usuario:/home/usuario# nmap -sP 10.0.224.*  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-05 17:18 CEST  
Nmap scan report for _gateway (10.0.224.1)  
Host is up (0.00011s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 10.0.224.2  
Host is up (0.000088s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 10.0.224.3  
Host is up (0.000072s latency).  
MAC Address: 08:00:27:DF:D9:EF (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.224.10  
Host is up (0.00020s latency).  
MAC Address: 08:00:27:47:FE:2F (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.224.50  
Host is up (0.00012s latency).  
MAC Address: 08:00:27:49:E5:87 (Oracle VirtualBox virtual NIC)  
Nmap scan report for usuario (10.0.224.6)  
Host is up.  
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.34 seconds  
root@usuario:/home/usuario#
```

```
root@usuario:/home/usuario# nmap -sP 10.0.224.0/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-05 17:19 CEST  
Nmap scan report for _gateway (10.0.224.1)  
Host is up (0.00017s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 10.0.224.2  
Host is up (0.00015s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 10.0.224.3  
Host is up (0.00015s latency).  
MAC Address: 08:00:27:DF:D9:EF (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.224.10  
Host is up (0.00019s latency).  
MAC Address: 08:00:27:47:FE:2F (Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.224.50  
Host is up (0.00019s latency).  
MAC Address: 08:00:27:49:E5:87 (Oracle VirtualBox virtual NIC)  
Nmap scan report for usuario (10.0.224.6)  
Host is up.  
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.09 seconds  
root@usuario:/home/usuario#
```


EJERCICIO 4 - Comprobar los puertos abiertos en un host de la red

> nmap W.X.Y.Z

Dependiendo de la seguridad de la IP que se escanee, puede que nos bloquee si lo hacemos de esa manera. Una forma más discreta de hacerlo que no deja registros en el sistema es así:

> nmap -sS W.X.Y.Z

Desde Ubuntu a la máquina Windows 10

```
Nmap scan report for 10.0.224.50
Host is up (0.00028s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
5357/tcp  open  wsapi
MAC Address: 08:00:27:49:E5:87 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.98 seconds
root@usuario:/home/usuario#
```

EJERCICIO 5 - Comprobar las versiones de los servicios que se ejecutan en los puertos

nmap -sV W.X.Y.Z

Desde Ubuntu a la máquina Windows 10

```
root@usuario:/home/usuario# nmap -sV 10.0.224.50
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-05 17:32 CEST
Nmap scan report for 10.0.224.50
Host is up (0.00026s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
5357/tcp  open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:49:E5:87 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 27.56 seconds
root@usuario:/home/usuario#
```

EJERCICIO 6 - Detectar S.O.

nmap -O W.X.Y.*

Desde Windows a los equipos de toda la red

```
Selecc... Seleccionar Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>nmap -O 10.0.224.*
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-05 17:46 Hora de verano romance
Nmap scan report for 10.0.224.1
Host is up (0.00042s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=10/5%OT=53%CT=1%CU=33743%PV=Y%DS=1%DC=D%G=Y%M=525400%T
OS:M=651EDA48%P=i686-pc-windows-windows)SEQ(SP=0%GCD=A3%ISR=54%TI=I%CI=I%II
OS:=RI%SS=0%TS=U)SEQ(SP=19%GCD=1%ISR=55%TI=I%CI=I%II=RI%SS=0%TS=U)SEQ(SP=1D
OS:%GCD=1%ISR=5C%TI=I%CI=I%II=RI%TS=U)SEQ(SP=21%GCD=1%ISR=5C%TI=I%CI=I%II=R
OS:I%TS=U)SEQ(SP=34%GCD=1%ISR=54%TI=I%CI=I%II=RI%SS=0%TS=U)OPS(O1=M5B4%O2=M
OS:5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=8000%W2=8000%W3=8000%W4=8000%
OS:W5=8000%W6=8000)ECN(R=Y%DF=N%T=FF%W=8000%O=M5B4%CC=N%Q=)T1(R=Y%DF=N%T=FF
OS:%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=N%T=FF%W=8000%S=0%A=S+%F=AS%O=M5
OS:B4%RD=0%Q=)T4(R=Y%DF=N%T=FF%W=8000%S=A%A=S+F=AR%O=%RD=0%Q=)T5(R=Y%DF=N%T
OS:=FF%W=8000%S=A%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=FF%W=8000%S=A%A=S+F=AR
OS:%O=%RD=0%Q=)T7(R=Y%DF=N%T=FF%W=8000%S=A%A=S+F=AR%O=%RD=0%Q=)U1(R=Y%DF=N
OS:%T=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=FF%CD
OS:=S)

Network Distance: 1 hop

Nmap scan report for 10.0.224.2
```